Revue Interventions économiques
Papers in Political Economy

59 | 2018
La nature sociale de la monnaie. Enjeux théoriques et portée institutionnelle

Les monnaies virtuelles décentralisées sont-elles des dispositifs d'avenir ?

Decentralized Virtual Currencies Are They Tools for the Future?

Ariane Tichit, Pascal Lafourcade et Vincent Mazenod

Édition électronique
URL : http://journals.openedition.org/interventionseconomiques/3771
DOI : 10.4000/interventionseconomiques.3771
ISBN : 1710-7377
ISSN : 1710-7377

Éditeur
Association d'Économie Politique

Référence électronique
Ariane Tichit, Pascal Lafourcade et Vincent Mazenod, « Les monnaies virtuelles décentralisées sont-elles des dispositifs d'avenir ? », *Revue Interventions économiques* [En ligne], 59 | 2018, mis en ligne le 01 janvier 2018, consulté le 14 juin 2019. URL : http://journals.openedition.org/interventionseconomiques/3771 ; DOI : 10.4000/interventionseconomiques.3771

Les monnaies virtuelles décentralisées sont-elles des dispositifs d'avenir ?

Decentralized Virtual Currencies Are They Tools for the Future?

Ariane Tichit, Pascal Lafourcade et Vincent Mazenod

Nous tenons à remercier chaleureusement les deux rapporteurs anonymes pour leurs remarques qui nous ont permis d'améliorer considérablement la première version de cet article, Clément Mathonnat pour ses précieuses relectures, ainsi que Cyril Fievet et Michaël Witrant pour leurs contributions.

1. Introduction

1 Les monnaies dites *virtuelles* ont connu un essor phénoménal ces dernières années, en particulier depuis l'apparition de Bitcoin. Elles sont appelées ainsi pour les distinguer des monnaies *électroniques* ou *numériques* qui ne sont qu'une version dématérialisée des devises traditionnelles, selon la directive européenne de 2009[1]. La Banque Centrale Européenne (BCE), dans son rapport 2012, définit les monnaies *virtuelles* comme un type de monnaie dématérialisée non régulée, créée et généralement contrôlée par ses développeurs, et utilisée et acceptée au sein des membres d'une communauté virtuelle spécifique. Parmi celles-ci[2], nous nous concentrons dans cet article sur celles qui sont convertibles avec d'autres monnaies. Celles-ci reposent souvent sur un principe de création et de gestion *décentralisé* basé sur des mécanismes cryptographiques, comme par exemple Bitcoin. Pour cette raison, elles sont en général qualifiées de *crypto-monnaies* ou de monnaies *virtuelles décentralisées*. Présentées de cette manière, elles semblent très éloignées d'autres monnaies dites "alternatives" ou "complémentaires" telles que les Systèmes d'Échanges Locaux (SELs), clubs de troc, banques de temps ou autres monnaies locales. Le premier objectif de cet article est de montrer qu'elles ont des points communs avec ces projets. Leurs caractéristiques intrinsèques cumulent notamment certains avantages des monnaies locales et les SELs en un seul objet monétaire et apportent des

solutions à certaines de leurs limites, même si des freins à leur utilisation existent également. À l'heure actuelle, l'élément essentiel qui les distingue est leur utilisation : partage de savoirs et lien social dans le cas des SELs, redynamisation des activités locales et lutte contre la spéculation pour les monnaies locales, et échanges et transferts à buts commerciaux et lucratifs pour les monnaies virtuelles décentralisées. Ces monnaies n'intéressent donc pas le même type de communautés. Le caractère social de la monnaie très marqué dans les projets SELs et les monnaies locales attirent de fait des personnes intéressées par l'Économie Sociale et Solidaire (ESS). À l'opposé, comme le soulignent Laurent et Monvoisin (2015), Dupré *et al.* (2015b) et Lakomsky-Laguerre et Desmedt (2015), les monnaies virtuelles décentralisées sont issues de philosophies libertarienne et anarchiste. Pour Weber (2014) elles incarnent également la concurrence monétaire chère à Hayek (1976) et à l'école autrichienne. Dès lors, ces monnaies attirent des chercheurs, citoyens et autres institutions s'intéressant aux nouvelles technologies, à l'open source, et voyant dans ces nouvelles monnaies la possibilité d'une véritable liberté de choix. S'il apparaît très clairement que les deux groupes se rejoignent sur la volonté d'une transformation systémique, ils s'opposent quant à la manière et aux outils du changement, ainsi qu'au type de système auquel ils veulent aboutir. Ces antinomies et les désaccords qu'elles engendrent apparaissent distinctement dans les publications émanant des deux groupes (voir Dupré *et al.*, 2015b, pour un article contre le Bitcoin et la publication[3] de Favier[4] en réaction, et De Vauplane, 2015, sur le blogue d'alternatives économiques[5] pour un article plutôt favorable à Bitcoin). Lakomsky-Laguerre et Desmedt (2015) et Desmedt et Lakomsky-Laguerre (2016), proposent quant à eux des analyses clarifiant les oppositions et discutent de la nature monétaire même de Bitcoin en partant d'une définition institutionnaliste de la monnaie.

2 La plupart des analyses institutionnalistes considère l'unité de compte comme la caractéristique fondamentale d'une monnaie (Ingham, 2004). Pour eux, comme pour Keynes (1930/1971), le fait de disposer d'un instrument de mesure de la valeur des choses est ce qui fait fondamentalement la différence entre une économie monétaire et une économie de troc. Ainsi, les institutionnalistes envisagent la monnaie comme une convention sociale, s'érigeant en institution de mesure de la valeur acceptée par tous lorsqu'une confiance suffisante est placée en elle (Aglietta et Orléan, 2002). Partant de ce principe, la théorie des systèmes de paiement développée par Cartelier (1991, 1996) définit la monnaie comme étant l'institution minimale permettant l'émergence et le fonctionnement d'une économie de marché décentralisée. Pour cela, tout système de paiement doit comporter, outre une unité de compte, une règle de mise en circulation des unités et une règle de paiement (c'est-à-dire de règlement des soldes). Appliquant cette grille de lecture au Bitcoin, Lakomsky-Laguerre et Desmedt (2015) montrent que si Bitcoin possède certaines des caractéristiques d'un système de paiement, il ne peut être considéré comme une institution monétaire à part entière. Ceci rejoint les travaux de Weber (2014) qui souligne les limites de la légitimité de Bitcoin, mais également la volatilité de son cours par rapport aux monnaies souveraines, qui ne lui permettent pas d'être une unité de mesure de la valeur des transactions réelles.

3 Cependant, ces analyses portent uniquement sur Bitcoin. Or, une grande diversification est en cours au sein des monnaies virtuelles décentralisées. Si les premières à apparaître après Bitcoin n'en étaient que des clones, certaines d'entre elles développent désormais des protocoles économes en énergie, plus utiles à la collectivité ou basés sur la coopération. D'autres se mettent au service de projets à valeurs proches de l'ESS. Le

deuxième objectif de cet article est ainsi de montrer que l'adoption de crypto-monnaies par les mouvements proches de l'ESS permettrait de fédérer deux communautés ayant pour projet de contester le système monétaire actuel. La fusion de ces courants pourrait ainsi créer un mouvement d'une ampleur suffisante pour commencer à représenter un véritable contre-pouvoir face aux structures dominantes.

4 Pour étayer ces propos, l'article est structuré en trois grandes parties. Dans la première nous montrons que les monnaies virtuelles décentralisées cumulent un certain nombre des points forts des monnaies locales et des SELs dans leur pouvoir transformateur et apportent des solutions à certaines de leurs faiblesses, tout en ayant évidemment leurs propres limites. Dans une deuxième partie, nous dressons un état de la diversification considérable des projets des crypto-monnaies ces dernières années et proposons une typologie. Enfin, dans la dernière partie, nous présentons une analyse de certains projets de monnaies virtuelles décentralisées portant des valeurs de l'ESS, signe d'une amorce de convergence entre les deux courants. Nous émettons toutefois certaines critiques sur ces dispositifs et proposons, en dernier lieu, une idée de crypto-monnaie géolocalisée avec fonte qui pourrait répondre à certaines limites rencontrées notamment par les monnaies locales dans leur définition de la proximité.

2. Monnaies virtuelles décentralisées de première génération, SELs et monnaies locales: points communs et divergences, points forts et limites

5 La première section de cette partie met en lumière des critères de distinction entre les monnaies virtuelles et les SELs et monnaies locales. Une seconde section souligne les caractéristiques des SELs et des monnaies locales qui favorisent ou limitent leur pouvoir transformateur et leur diffusion, et montre que les crypto-monnaies réunissent certains des points forts de ces projets et apportent des solutions à certaines de leurs limites, même si des freins à leur utilisation existent également.

2.1. Points communs et divergences entre les SELs, les monnaies locales complémentaires et les crypto-monnaies

6 L'explosion de la diversité des formes monétaires depuis les années 2000 a donné lieu à un large mouvement de recherche d'une classification claire de ces différents objets, amorcé par les travaux de Kennedy et Lietaer (2004) et de Bode (2004) et prolongés depuis par Blanc (2011), Schroeder (2011), Slay (2011), Martignoni (2012), Bindewald *et al.* (2013), Seyfang et Longhurst (2013), Dupré *et al.* (2015b). Toutefois, la plupart de ces travaux reposent sur des critères de classification choisis *a priori* par les chercheurs en fonction de leurs connaissances, leurs intérêts d'études et de leur propre vision subjective des projets. D'autre part, beaucoup d'entre eux ne portent pas sur l'ensemble des formes monétaires, mais essentiellement sur les projets de types monnaies locales et SELs, laissant la plupart du temps les monnaies virtuelles de côté. Les divergences philosophiques soulignées en introduction expliquent que la communauté des chercheurs se divise en fonction des types de monnaies auxquels elle s'intéresse et que peu de typologies embrassant l'ensemble des formes monétaires existent. Toutefois, une classification proposée par Dupré *et al.* (2015a) sur quelques monnaies représentatives inclus le Bitcoin. Les critères

de différenciation qu'ils retiennent sont les fonctions remplies par la monnaie (échange, épargne, moyen de paiement et spéculation) et les valeurs portées par les projets : politiques, sociales et écologiques. Sur la plupart des critères retenus par les auteurs, le Bitcoin s'oppose aux SELs et au Sol-violette[6].

7 Cependant, selon Tichit *et al.* (2016), cette typologie souffre, comme toutes les autres, de la subjectivité des critères retenus par les chercheurs. Afin de contourner ce problème, ces auteurs proposent une catégorisation endogène, en utilisant comme sources d'informations les pages web des monnaies "non-bancaires"[7]. L'avantage de cette méthodologie est d'utiliser les sources d'information émanant des concepteurs des projets eux-mêmes et de leur façon de les présenter, ce qui évite de recourir à des hypothèses préalables sur les facteurs régissant les taxonomies. Grâce à cette approche, les auteurs aboutissent à une typologie des monnaies alternatives actuelles en trois grandes catégories : les clubs de troc et autres SELs, les monnaies locales complémentaires et les monnaies virtuelles de type Bitcoin. Ils en déduisent deux critères de distinction principaux : la dépendance/indépendance vis-à-vis de la monnaie standard (pour la création et la circulation) et les valeurs et fonctions que les projets de monnaie servent. L'avantage de cette typologie est de proposer des caractéristiques différenciatrices très simples et englobantes. Partant des critères de classification de Tichit *et al.* (2016), nous proposons ici un approfondissement des points communs et des divergences entre les monnaies virtuelles décentralisées à la Bitcoin, les monnaies locales et les SELs. Les principaux éléments de distinction sont synthétisés dans le tableau suivant :

Tableau 1. Critères de différenciation monnaies virtuelles/SELs/monnaies locales

Types de monnaies	Valeurs sociales, environnementales, solidaires, but non lucratif	Convertibilité avec les monnaies standards	Création d'unités adossées aux monnaies standards	Circulation dans la sphère marchande	Fiscalisation	Circulation sous forme dématérialisée	Variabilité de la valeur par rapport aux monnaies standards
Monnaie locale complémentaire	oui	oui	oui	oui	oui	non	non
SELs	oui	non	non	non	non	pas de circulation en tant que telle	pas de convertibilité
Monnaies virtuelles décentralisées type Bitcoin	non	oui	non	oui	oui partiellement	oui	oui

8 Le facteur fondamental qui distingue les monnaies locales et les SELs des monnaies virtuelles décentralisées de première génération à la Bitcoin sont les valeurs défendues par les projets. En caricaturant, la liberté, l'accumulation, l'enrichissement et la spéculation sont favorisés par les crypto-monnaies décentralisées, et le partage, la solidarité, le but non lucratif et la lutte contre la spéculation sont défendus par les SELs et les monnaies locales. Pour ce qui est des autres caractéristiques, la section suivante commente les différents champs sous le prisme des points forts et faibles des projets dans leur pouvoir transformateur du système actuel. Elle montre aussi que les crypto-

monnaies concentrent certains avantages d'autres monnaies alternatives et apportent des solutions à certaines de leurs limites, même si des freins à leur utilisation existent.

2.2. Points forts et limites des SELs, des monnaies locales et des crypto-monnaies

9 Une première grande différence entre les SELS, les monnaies locales et les crypto-monnaies est leur degré d'autonomie vis-à-vis des monnaies standards. Une unité de monnaie locale ne peut en effet circuler qu'à la condition d'avoir été échangée contre une unité de monnaie souveraine. Il faut donc au préalable qu'une unité de devise standard ait été émise par une banque commerciale avant qu'elle ne puisse être transformée et circuler sous forme de monnaie locale. En ceci elles ne sont pas dotées d'une création autonome d'unités et ne remettent donc pas fondamentalement en question la création monétaire privée par le crédit, contrairement aux SELs et aux crypto-monnaies. En effet, ces derniers sont indépendants des monnaies standards, même si le processus de production d'unités diffère dans chacun des projets. Pour les SELs, la création monétaire n'est présente qu'à travers le crédit offert aux participants, soit par une possibilité de dette plafonnée, soit par l'attribution d'une quantité initiale d'unités à l'entrée dans le réseau. Les échanges ne donnent ensuite lieu qu'à un exercice comptable, ne créant pas de nouvelles unités[8]. Dans le cas des crypto-monnaies, les unités sont créées pour récompenser la contribution des membres à la validation des échanges. Elles seules offrent donc un protocole de création d'unités sans lien avec les banques privées.

10 Une autre différence tient à la valeur de la monnaie. La monnaie interne des SELs n'a pas d'équivalence avec la monnaie standard et n'est pas convertible, contrairement aux crypto-monnaies et aux monnaies locales. Comme l'étudient notamment Dokhan (2000) et Laacher (2002), il existe une hétérogénéité dans le fonctionnement des plus de 380 SELs existant en France, mais en général, l'étalon de valeur est l'heure de travail humain quel que soit le type de service offert. Ils remettent donc foncièrement en question la hiérarchisation des valeurs présente dans le système actuel. Dans le cas des crypto-monnaies, la valeur dépend de la confrontation de l'offre et la demande. Le cours du Bitcoin vis-à-vis des devises standards est très fluctuant[9]. Il a atteint une valeur record en 2014, avant de connaître une forte baisse suite à l'affaire de l'attaque Mt.Gox. Début 2017, il a dépassé sa valeur maximale de 2014. Cette volatilité de Bitcoin peut constituer un frein à son utilisation et à la confiance nécessaire pour accéder au statut de monnaie à part entière (voir Lakomsky-Laguerre et Desmedt, 2015 et Weber 2014). Cette question de la variation de la valeur est absente des monnaies locales, qui sont fixées à parité unitaire avec les monnaies souveraines, ce qui leur confère dès lors l'avantage de la stabilité. Mais un frein à leur utilisation est le fait de circuler essentiellement sous forme papier. Ceci est lié au fait que pour exister sous format électronique elles doivent demander une exemption auprès de l'ACPR (Autorité de Contrôle Prudentiel et de Résolution)[10] en France, ce que seul l'Eusko a réussi à obtenir en mars 2017[11]. Toutefois, même si une circulation en version électronique des monnaies locales peut faciliter leur utilisation, ceci ne leur confère pas d'existence autonome vis-à-vis des monnaies standards.

11 Une troisième différence tient à la question de la fiscalisation des transactions. Les échanges au sein des SELs ne sont pas soumis à taxation, contrairement à ceux effectués en monnaies locales. Ceci freine alors leur expansion, car ils entrent de fait en concurrence avec les activités marchandes. Ils sont en conséquence tolérés par les

instances officielles tant qu'ils ne dépassent pas un certain volume d'échanges et ne génèrent pas un manque à gagner fiscal trop important. En grossissant, le risque serait de se faire interdire pour travail au noir ou échanges non déclarés. Par la contrainte légale, les SELs sont ainsi voués à demeurer de petites structures. En circulant dans l'économie marchande, comme les monnaies locales, les crypto-monnaies ne rencontrent pas cette limite intrinsèque. En effet, dès que des unités de monnaies virtuelles décentralisées sont échangées contre des devises standards ou servent à des échanges dans l'économie réelle, elles sont assujetties aux mêmes taxes et impôts que les autres moyens de paiement. C'est d'ailleurs la possibilité de taxer les transactions en bitcoins qui a motivé le gouvernement allemand, en 2013, à reconnaître Bitcoin comme une monnaie privée. Le Japon la considère aussi officiellement comme monnaie depuis le 1er avril 2017. Il est de ce fait probable que ce type de monnaie virtuelle soit reconnu légalement dans les années qui viennent dans de nombreux pays.

12 Comme nous venons de le voir, les crypto-monnaies cumulent un certain nombre de points forts des monnaies locales et des SELs : elles sont par essence dématérialisées donc faciles d'utilisation, circulent dans l'économie marchande et les unités sont créées sans lien avec les monnaies traditionnelles. Au-delà de ça, elles ont un avantage supplémentaire que ne possèdent ni les SELs ni les monnaies locales complémentaires: leur caractère décentralisé qui les rend très difficilement contrôlables par les autorités. En effet, comme chaque participant possède l'intégralité de l'information du système, si des autorités saisissent le matériel de certaines entités créatrices d'unités, n'importe quel autre participant, n'importe où sur la planète, peut continuer à faire fonctionner les échanges et le réseau. À l'inverse, les SELS et monnaies locales, de par leur centralisation, peuvent être très facilement interdits et surveillés. Comme le souligne Lietaer (2013) l'histoire regorge d'interdictions de projets monétaires alternatifs prometteurs dans leur potentiel de transformation systémique. La prohibition de l'expérience de Wörgl en Autriche pendant la grande récession (Kennedy, 1995) ou de certaines initiatives françaises dans les années 30 et 50 (voir Laacher, 1998) est emblématique de ce pouvoir étatique de mettre fin aux expérimentations aux résultats très encourageants. Les crypto-monnaies ont par conséquent comme avantage d'être beaucoup plus difficilement contrôlables, du fait de leur caractère distribué.

13 Toutefois, elles se heurtent elles-mêmes à certaines limites. Les protocoles utilisés par les crypto-monnaies sont assurément difficiles à comprendre pour le commun des mortels, ce qui implique de faire confiance à la technologie et à la transparence de l'information. De plus, comme les valeurs détenues en crypto-monnaies ne sont régulées par aucune institution, il est difficile d'attirer des personnes qui ne s'interrogent pas sur le fonctionnement ni les conséquences du système monétaire et financier actuel, et donc sa fiabilité véritable. Leur grande volatilité génère également une certaine méfiance de la part des usagers potentiels.

14 Se pose également la question de ce qu'il est vraiment possible d'acheter avec ces monnaies, pour qu'elles ne restent pas cantonnées à la seule fonction de réserve ou d'échanges de biens et services dématérialisés. La thésaurisation semble d'ailleurs prendre de l'ampleur lorsque la menace de crise monétaire et financière se fait plus pressante, par exemple en 2015 en Grèce[12]. Weber (2014) souligne d'ailleurs qu'elle est la fonction principale de Bitcoin, celui-ci ne pouvant guère être considéré comme une monnaie multifonctionnelle tant les deux autres fonctions essentielles que sont l'unité de compte et le moyen de paiement sont encore peu présentes. Cette limite des crypto-

monnaies est toutefois en train d'être dépassée, car de plus en plus de commerçants dans le monde acceptent les bitcoins. En 2015 plus de 100 000 commerces[13] seraient concernés. En outre, des moyens de paiement de plus en plus accessibles et peu onéreux se développent, comme Shift[14], la première carte américaine de paiement en bitcoins, utilisable dans tous les commerces du monde acceptant les cartes Visa, c'est-à-dire plus de 38 millions. D'autres versions de ce type de cartes sont en train de se développer pour englober d'autres crypto-monnaies, comme prypto[15], ou des outils facilitant la conversion des crypto-monnaies entre elles, comme coinbase[16]. La plupart de ces modes de paiement fonctionnent comme des convertisseurs de crypto-monnaies en monnaies conventionnelles. Ils permettent ainsi de contourner le problème de fixation de prix en crypto-monnaies pour les vendeurs, étant donné que les prix comme les paiements se font en monnaies standards, le risque de change étant assumé par les acheteurs. Ceci ne change donc rien pour les commerçants, qui ne s'aperçoivent même pas que des crypto-monnaies ont été dépensées lors de la transaction. Ce domaine est donc en pleine expansion et vise à augmenter le taux de pénétration des monnaies virtuelles décentralisées dans l'économie réelle.

15 Cette première partie s'est attachée à analyser l'apport potentiel de la première génération de cryto-monnaies comparativement aux SELs et aux monnaies locales. La prochaine partie présente leur évolution, de l'apparition du Bitcoin à l'émergence d'une multitude d'Altcoins, dont certains se rapprochent de l'ESS.

3. Diversification des monnaies virtuelles décentralisées: vers l'émergence de nouveaux paradigmes

16 Cette partie est structurée en deux sous-sections. La première rappelle les fondements des crypto-monnaies virtuelles centralisées et présente la révolution Bitcoin, première monnaie décentralisée. La seconde sous-section décrit ensuite les innovations qu'apporte la diversification de ces formes monétaires, dont certaines conduisent à un changement de paradigme.

3.1. Des crypto-monnaies centralisées au Bitcoin

17 Le premier protocole cryptographique visant à assurer la sécurité des transactions et le respect de la vie privée des utilisateurs d'une monnaie numérique a été proposé par Chaum en 1983. Il s'inspire des propriétés des monnaies fiduciaires qui par essence assurent ces deux principes. Dreier *et al.* (2015) déterminent trois catégories principales de fonctionnalités que doivent garantir les monnaies électroniques:

- *La monnaie doit être non falsifiable (non-forgeable)*: Il ne doit pas être possible de créer de la monnaie par un utilisateur non habilité à une telle action par le système.
- *Il ne doit pas être possible de dépenser deux fois une même unité :* Une monnaie dématérialisée étant plus facile à dupliquer, il faut alors interdire la possibilité de dépenser plusieurs fois la même unité. Il faut également pouvoir identifier le fraudeur si cela se produit et s'assurer qu'une personne honnête ne puisse être accusée à tort.
- *La vie privée doit être respectée*: il existe deux versions de ce principe. L'anonymat *faible* garantit qu'il n'est pas possible de savoir qui a effectué une transaction. L'anonymat *fort*, en

plus de l'anonymat faible, assure qu'il n'est pas possible de savoir si deux transactions différentes ont été faites par la même entité.

18 Cependant, les protocoles développés jusque-là avec ces propriétés ne l'étaient que dans le cadre de systèmes centralisés. Or, en 2008, la création du Bitcoin par Satoshi Nakamoto propose pour la première fois un système *décentralisé* garantissant ces principes, ce qui est une révolution. Celui-ci fonctionne sans autorité centrale pour la création de la monnaie et la gestion des transactions. La sécurité de ce système repose sur une architecture où chaque utilisateur possède une clé publique (connue de tous) et une clé secrète (connue uniquement de son propriétaire). Ces clés permettent à chacun de signer électroniquement des transactions, mais aussi de pouvoir vérifier la validité de ces signatures. La création de nouveaux bitcoins est partie intégrante du système et récompense les personnes qui assurent son fonctionnement. Ces personnes qui valident les transactions effectuées par les utilisateurs sont appelés *mineurs.* L'effort produit, en termes de calculs effectués par les mineurs, donc d'énergie en Kilos Watts dépensés, est appelé *preuve de travail*. Chaque fois qu'un mineur valide un ensemble de transactions, en énumérant des nombres jusqu'à trouver le nombre résolvant l'objectif courant fixé dynamiquement par le système, il crée des bitcoins qu'il obtient ensuite en rémunération. Les mineurs font donc fonctionner le système et déterminent la fréquence à laquelle les transactions sont validées. Ce mécanisme s'appelle la *Block Chain*[17]. Une autre caractéristique de Bitcoin est que l'ensemble des transactions et des validations sont publiquement vérifiables par tout le monde, ce qui est un élément crucial pour créer la confiance des utilisateurs dans le système. Enfin le nombre de bitcoins est borné par le protocole lui-même : il n'y aura que 21 millions de bitcoins créés. Cette limite est obtenue en réduisant la rémunération (donc le nombre d'unités créées) liée à la validation des transactions. Ainsi la récompense baisse avec le nombre d'unités déjà créées. Il faut donc valider plus de blocs pour gagner autant de bitcoins, si bien que les mineurs se sont peu à peu regroupés en fermes de minage (sorte de coopératives) afin d'être plus efficaces et surtout pour garantir un revenu à chaque mineur. Or, si une personne possède plus de 51% des ressources de minage, il lui est possible de contrôler la création de la monnaie. Effectivement cette ferme de minage validera plus de transactions que les autres et, comme seule la chaîne de transactions la plus longue est retenue, pourra valider les transactions de son choix et de fait totalement contrôler les échanges. C'est une des limites intrinsèques du Bitcoin, qui ne garantit pas une décentralisation absolue.

19 Enfin Bitcoin est souvent considéré comme anonyme, mais il s'agit d'une forme particulière d'anonymat. L'identité des possesseurs des clés publiques n'est en effet pas nécessaire pour assurer la sécurité des transactions. Le monde entier peut voir qu'un montant est transféré d'un compte à un autre, sans qu'il soit possible d'établir un lien avec des personnes physiques ou morales. Toutefois, au moment où une personne entre ou sort du système, par exemple par un échange avec une autre monnaie, l'anonymat doit être levé, au moins auprès de l'organisme de change, et l'ensemble des transactions associées à cette clé peut alors être tracé.

20 Fort de son succès et parce qu'il est aisé de mettre en place une nouvelle monnaie reposant sur Bitcoin dont le protocole est open source, de nombreux clones de Bitcoin ont vu le jour. Il existe à l'heure actuelle plus de 269 crypto-monnaies référencées[18] dont certaines, comparativement au Bitcoin, représentent des avancées techniques telles qu'elles peuvent être considérées comme de nouveaux changements de paradigme (Tschorsch et Scheuermann, 2016).

3.2. Jusqu'à des milliers d'Altcoins[19] dont certains ouvrant sur de nouveaux paradigmes

21 Nous proposons ici une classification de ces projets en quatre grandes catégories, selon leurs objectifs et caractéristiques techniques. La première correspond aux Altcoins que Fievet (2014) classe comme "pourris" c'est-à-dire ceux conçus à la "va-vite", souffrant de défaillances conceptuelles et ne visant qu'à enrichir ses propriétaires. Ils sont, selon Fievet (2014) très vite reconnus et dénoncés par la communauté des *bitcoiners*, et ont de fait une durée de vie très courte.

22 Il y a ensuite la catégorie des monnaies qui reposent sur le même principe de la *Block Chain* introduite par Bitcoin, mais qui visent à fédérer une communauté, en ne circulant qu'à l'intérieur d'un groupe d'utilisateurs bien précis ou servant à des achats et ventes spécifiques. Par exemple, Guncoin[20] propose une monnaie pour l'achat et la vente d'armes, ou encore Potcoin[21] qui permet d'acheter de la marijuana à usage thérapeutique. D'autres exemples de ce type de monnaies sont donnés dans Fievet (2014), p.23-24, tels que les Rainbowcoins pour fédérer les communautés gaies et lesbiennes, ou le Pokercoin pour les joueurs de poker. Toutefois une des principales critiques adressée à Bitcoin et à ses clones est l'impact sur l'environnement, car participer à la *Block Chain* engendre des calculs énergivores qui n'apportent rien d'autre que de valider les transactions du système.

23 Une troisième catégorie d'Altcoins vise ainsi à rendre les principes de minage plus économes et pour certains également plus utiles. Nous proposons de diviser cette catégorie en trois sous-ensembles: le premier concerne des avancées techniques pour rendre la création d'unités par la preuve de travail moins énergivore, sans remettre fondamentalement en question son fonctionnement ni son principe. Ceci est le cas par exemple de Dogecoin[22] ou Litecoin[23]. Ces monnaies offrent des temps de validation de transactions en moyenne plus courts (2 minutes trente pour Litecoin et 1 minute pour Dogecoin au lieu de 10 minutes pour Bitcoin). Dans la même direction, FawkesCoin a été proposé par Bonneau et Miller (2014) sur un plan théorique sans être déployé, où seules des primitives cryptographiques utilisant des clés symétriques sont utilisées, ce qui rend les calculs plus rapides. Le second sous-ensemble d'avancées techniques met le processus de validation des transactions au service de tâches plus utiles. Par exemple King (2013) propose Primecoin[24] qui remplace la preuve de travail de Bitcoin par le calcul des chaînes de Cunningham sur les nombres premiers. Aussi, la découverte de ces chaînes fait avancer la recherche en mathématiques tout en validant des transactions. D'autres comme Gridcoin[25], Curecoin[26] ou encore Foldingcoin[27] proposent de mettre les calculs de validation des transactions au service de la science ou de la médecine, en participant à l'analyse du fonctionnement des protéines par exemple dans le cas de Curecoin.

24 Une dernière catégorie d'Altcoins propose des protocoles pour valider les transactions qui ne sont pas basés sur la preuve de travail. Par exemple Peercoin[28], proposé par King et Nadal (2012) repose sur *une preuve de participation (proof of stake)*. Par opposition à Bitcoin, où il faut avoir une grande puissance de calcul pour tester de nombreuses valeurs pour résoudre un objectif de hachage[29], ici, plus une personne attend plus elle a de chances d'atteindre l'objectif nécessaire pour valider une transaction. Ensuite en cas d'égalité entre plusieurs participants ayant atteint l'objectif, celui ayant les unités les plus âgées l'emporte. Cette alternative permet de rendre plus équitable et démocratique le processus

de validation en faisant participer chacun sans consommer de grandes quantités d'énergie. Pour éviter que les mineurs restent passifs et attendent hors ligne que leurs unités prennent de la valeur, Reddcoin encourage les transactions en pénalisant les mineurs passifs en introduisant la notion de *rapidité de preuve de participation* (*proof of stake velocity*). Dans la même direction Bentov *et al.* (2014) proposent quant à eux une *preuve d'activité (proof of activity)* pour récompenser les mineurs les plus actifs (ceux restant le plus longtemps en ligne). Enfin Miller et al (2014) proposent Permacoin[30], où un mineur doit prouver qu'il stocke bien des données dans un réseau pair-à-pair en effectuant une *preuve de "récupération" (proof of retrievability)*. Après la proposition de Burstcoin[31], d'utiliser l'espace disque comme ressource pour le minage en faisant une *preuve de capacité (Proof of Capacity)*, Park et al (2015) ont proposé SpaceMint, qui améliore les mécanismes cryptographiques introduits dans la preuve d'espace (*proof of space*) proposée par Dziembowski *et al.* (2015). L'idée est de mettre à disposition de l'espace de stockage et d'être capable de le prouver pour être récompensé. Ce processus offre de nouvelles perspectives pour ne plus gaspiller de l'énergie et offrir des moyens de stockage distribués.

25 À travers cette présentation de l'évolution des monnaies virtuelles décentralisées vers une diversité, il apparaît très nettement que certaines d'entre elles partagent un certain nombre de valeurs chères aux mouvements de l'ESS: la volonté de rendre la validation de transactions utile à la communauté, pour Curecoin ou Primecoin, ou de baser les principes mêmes de la création d'unités sur des valeurs de participation à une communauté (pour Peercoin) ou de partage (pour Burstcoin ou Spacemint). Ces Altcoins nous semblent donc potentiellement détenir des caractéristiques ouvrant la voie à l'utilisation des crypto-monnaies dans le champ des activités de l'ESS. Cependant, les initiatives dans ce sens sont encore peu développées et les premières tentatives, qui font l'objet de l'analyse de la troisième partie de cet article, sont encore sujettes à de nombreuses limites et critiques. La fin de la dernière partie propose ensuite quelques idées théoriques qui pourraient permettre de dépasser certaines d'entre elles.

4. Émergence de crypto-monnaies au service de l'ESS et proposition d'un principe de fonte géolocalisée

26 Comme évoqué en première partie, les crypto-monnaies cumulent en un seul projet monétaire certaines forces transformatrices des monnaies locales et des SELs. En effet, elles permettent d'être indépendantes du système bancaire pour la création et la circulation monétaire, sont présentes dans le système marchand et sont de fait dématérialisées, ce qui rend potentiellement leur adoption et leur diffusion plus simples. Elles sont par ailleurs décentralisées, ce qui rend leur contrôle par les autorités beaucoup plus difficile. Des avancées théoriques permettent par ailleurs de les rendre moins énergivores et plus utiles pour la collectivité, ce qui les rapproche des valeurs de l'ESS, dont elles étaient, jusqu'à présent, plutôt éloignées. Dans cette partie, nous focalisons notre attention sur deux projets de monnaies virtuelles décentralisées en cours de déploiement visant à contribuer à une transformation de la société. Le premier est une monnaie au service d'un système coopératif mondial. Le second propose un principe au croisement d'une monnaie locale et d'un revenu de base. Après avoir présenté ces projets et souligné leurs limites dans une première sous-partie, nous proposons une idée de

crypto-monnaie géolocalisée fondante qui pourrait remplacer la notion très imparfaite de "proximité" qu'utilisent actuellement les monnaies locales complémentaires.

4.1. Analyse de deux projets de crypto-monnaies à vocations sociale et solidaire

27 La première monnaie mondiale au service de la coopération est le Faircoin, monnaie officielle de la plateforme coopérative mondiale Faircoop. Cette structure a fait couler beaucoup d'encre en particulier du fait de son fondateur Duran présenté comme un militant anti-capitaliste et libertaire révolutionnaire[32]. Faircoop est une monnaie "*conçue comme une économie "post-capitaliste", fondée sur la coopération et la culture du logiciel libre*" (Desmedt et Lakomsky-Laguerre, 2016, p.4.), ce qui fait ainsi de Faircoin la première monnaie virtuelle décentralisée au service de ce type de système. Apparue en 2014, cette crypto-monnaie a distribué 50 millions d'unités en mars 2014, pendant 3 jours, gratuitement à ceux qui s'étaient inscrits sur le site du Faircoin. Il a ensuite suffi à ces derniers de conserver leurs faircoins pendant vingt et un jours pour en recevoir automatiquement de nouveaux, en proportion de leur capital initial. Cependant, quelques semaines après une forte hausse, le cours s'est effondré. Le créateur de Faircoop épaulé par un informaticien ont alors proposé à la communauté de prendre collectivement le contrôle de cette monnaie sinistrée, de la faire évoluer et de la mettre au service de Faircoop[33]. D'un point de vue technique, Faircoin, dans sa deuxième version[34] se base sur des participants de confiance qui valident les transactions via une *preuve de coopération (proof-of-cooperation).* Ceci diminue considérablement les dépenses énergétiques pour la validation des transactions, défaut qu'avait la première version, car elle reposait sur Bitcoin. Dans la seconde version, les participants qui valident les transactions doivent être connectés et actifs. Une transaction n'est effective que lorsqu'il y a accord de la majorité des valideurs actifs. En contrepartie, les valideurs sont rémunérés par une taxe sur les transactions. Il est à noter que ce système ne génère plus de nouvelles unités de monnaie, mais propose un moyen distribué de gérer les transactions par des acteurs rémunérés. Cela suppose d'avoir confiance dans plus de la moitié des valideurs actifs, car sinon ils peuvent se mettre d'accord pour ne valider que les transactions de leur choix. Le montant des rémunérations et le choix des valideurs sont fixés par les administrateurs de la monnaie ce qui a une grande influence sur sa stabilité. Par ailleurs, il n'est possible à l'heure actuelle de se procurer des Faircoins qu'en changeant des unités d'autres crypto-monnaies ou d'autres devises sur certaines plateformes d'échange. Elle ne se caractérise donc plus par une création de monnaie sur la base d'un protocole de validation des transactions, mais s'apparente plutôt à une monnaie locale, définie non par un périmètre géographique, mais par une utilisation au sein d'une communauté fédérée autour de la Faircoop.

28 Un autre projet de monnaie virtuelle décentralisée proche des valeurs portées par l'ESS a vu le jour : Duniter. D'un point de vue théorique, il vise à la création d'une monnaie dite libre (*freecurrency*). Ce concept, très controversé et sujet à de nombreuses critiques, repose sur la Théorie Relative de la Monnaie (TRM) développé par Laborde (2010)[35] qui vise à assurer quatre libertés fondamentales[36] : 1) la liberté de choix de système monétaire, 2) la liberté d'accès aux ressources 3) la liberté d'évaluation et de production de valeurs 4) la liberté des échanges. Le principe fondamental est que le seul fait d'exister dans le système permet la création de la monnaie et non pas une preuve de travail ou de

participation. Le fait d'exister permet d'être créateur à chaque période de temps fixé d'un Dividende Universel (DU) ce qui est très proche du principe de revenu de base. La différence fondamentale réside dans le fait que chaque participant génère lui-même une fraction fixe de la masse monétaire. Le Sou mayennais, une expérience française de monnaie virtuelle locale basée sur la TRM est le premier projet, à notre connaissance, utilisant Duniter. Ce projet pionnier, lancé le 1er octobre 2016, se heurte pour le moment à de nombreuses difficultés techniques dans sa mise en œuvre. Le premier problème de l'application de la TRM est l'assurance qu'une personne n'existe qu'une seule fois. En effet, puisque le système ne garantit aucunement la possession d'une unique clé pour chaque utilisateur, rien n'interdit de se créer plusieurs clés privées donc plusieurs existences et par là de toucher plusieurs DU. Afin de pallier ce problème, le protocole impose un nombre minimum $k=5$ de signatures de membres pour qu'une nouvelle identité soit acceptée dans le réseau. Mais cette mesure n'est pas suffisante, car k membres malveillants peuvent signer autant de membres fictifs qu'ils le souhaitent et se partager autant de DU qu'ils auront créé de fausses identités. Dans un système distribué, ceci est une limite connue comme l'ont montré Lamport *et al.* (1982). Une solution possible à ce problème est d'avoir une autorité de confiance qui validerait l'existence des participants, mais cela irait à l'encontre du principe de la TRM qui rejette une autorité centrale, d'où le choix fait dans Duniter que tous les membres constituent la toile de confiance. Mais comment assurer que de fausses identités n'entrent jamais? C'est une question qui reste ouverte, comme le reconnaissent ses concepteurs qui sont à la recherche d'un compromis mathématique acceptable entre sécurité et praticalité[37].

29 Outre cette question de la sécurité, les monnaies libres ne peuvent pas être mises en circulation à partir d'une masse monétaire nulle et sans utilisateurs. Le principe est donc de constituer au préalable d'un réseau ad-hoc et un capital arbitraire initial afin d'amorcer le système. C'est d'ailleurs exactement ce qu'a fait Faircoin[38] dans sa seconde version, et ce que fait actuellement le Sou mayennais. Il compte à l'heure actuelle 100 membres, qui créent régulièrement leurs DU, peuvent faire des échanges entre eux, et tester le système. Pour le moment le Sou, dans sa version test, n'a pas encore d'utilisation dans l'économie réelle et n'est pas convertible avec les autres monnaies. Le Sou vise par ailleurs à favoriser l'économie locale sur les mêmes principes que les monnaies locales classiques tout en assurant un revenu de base sans recours aux euros. À cette fin il est limité géographiquement au territoire de la Mayenne[39]. Outre les limites techniques et théoriques que nous avons soulignées précédemment, il se pourrait que le Sou ouvre un champ de possibles à de nombreuses autres monnaies locales et à la mise en œuvre d'un revenu de base. Mais il annonce clairement que son périmètre de circulation exact dépendra *in fine* de la localisation géographique des participants au réseau. Ceci nous conduit à proposer une définition du local que permettent les monnaies dématérialisées et qui nous semble offrir des solutions à certains des problèmes rencontrés par les monnaies locales.

4.2. Une proposition de monnaie avec définition du local par une fonte géolocalisée

30 Un des objectifs des monnaies locales est de favoriser l'économie de proximité. Mais comment définir ce qui est considéré comme "local" ? Pour des raisons purement pratiques et légales, elles basent leur zone d'utilisation sur les limites des départements.

Or, ceci nous semble une définition assez contraignante et pas nécessairement pertinente du local, car pour certaines zones proches d'une frontière départementale, il pourrait être plus cohérent d'utiliser la monnaie locale du département voisin, en fonction du bassin de vie fréquenté par la personne. Or, les crypto-monnaies dématérialisées peuvent permettre de mettre en œuvre une définition de la localité plus cohérente. En effet, il est possible d'utiliser un principe de géolocalisation cumulé à une fonte pour assurer une incitation à la consommation de proximité. Le principe de monnaie fondante a été conceptualisé par Gesell (1948). Il correspond à une dévalorisation de la monnaie (une perte d'un pourcentage de sa valeur), lorsqu'elle ne circule pas. Ceci a pour but de décourager l'accumulation et inciter à la circulation de la monnaie, créatrice de richesses. Nous appliquons ici cette idée non pas à la thésaurisation, mais à la distance géographique, afin de favoriser la dépense de proximité. L'idée est la suivante. Chaque unité de monnaie possède en plus de ses propriétés fiduciaires, une information quant à son lieu et sa date d'émission (ce lieu est celui enregistré par géolocalisation de la personne au moment où elle reçoit des unités, soit suite à une transaction, soit lors de la création des unités). Chaque fois qu'une unité monétaire est échangée, ses caractéristiques sont mises à jour avec les coordonnées (lieu, date) de la dernière transaction. Ces données servent ensuite à déterminer la zone d'utilisation de la monnaie, et à y appliquer un système de fonte géographique pour assurer une incitation à la dépense de proximité. Par exemple dans un rayon de 100 km autour du lieu d'émission ou du dernier lieu d'échange, la monnaie aurait pleine valeur, au-delà de 100 km elle en perdrait un certain pourcentage, au-delà de 200 km un pourcentage plus élevé, etc., jusqu'à un point au-delà duquel elle n'aurait plus aucune valeur. L'utilisation de manière sécurisée des coordonnées GPS de l'acheteur et du vendeur permettent de réaliser cette proposition. Cette géolocalisation favorise l'économie locale et nous semble plus pertinente que la définition selon une zone géographique administrative, par essence imparfaite, qu'utilisent actuellement les monnaies locales.

31 La date de délivrance de la monnaie permet également d'ajouter une dévalorisation lorsqu'elle n'est pas utilisée depuis un certain temps. Ceci correspond au concept de fonte de Gesell (1948). Même si ce principe a de nombreuses vertus théoriques (favoriser la circulation et générer des ressources pour financer la gestion du système), de nombreuses monnaies locales ne la mettent pas en œuvre[40], notamment pour des raisons pratiques de mise en place sur des monnaies papier (timbres à coller dans le cas du Chiemgauer allemand, billets à durée de vie limitée pour la Roue en Provence, etc.). Il nous semble dès lors que les protocoles de crypto-monnaies basés sur un système d'horodatage sécurisé permettent de dépasser ce problème purement pratique en incluant le principe de fonte dans les mécanismes intrinsèques du fonctionnement de la monnaie.

32 Enfin, pour que l'épargne reste une éventualité, il est possible de n'appliquer la fonte temporelle qu'à un pourcentage de la monnaie détenue par les agents (la moitié par exemple). Si les unités sont créées mensuellement, la moitié des unités n'ayant pas été dépensées à la fin du mois pourraient perdre toute ou partie de leur valeur. Dans un tel système si aucun échange n'a lieu, la moitié de la monnaie émise disparaît à chaque période. Afin d'éviter cela et de conserver une masse monétaire stable, les pertes de valeur pourraient servir à rémunérer les personnes validant les transactions. Sur le même principe, comme souligné précédemment, la fonte géographique pourrait avoir la même utilité. Aussi, les personnes ne souhaitant pas dépenser tout leur revenu, et celles les dépensant loin de leur lieu de vie contribuent au fonctionnement du système. Bien

évidemment la mise en œuvre technique d'une telle monnaie nécessite de nombreux développements.

5. Conclusion

33 Les monnaies virtuelles décentralisées sont à l'heure actuelle en plein essor et commencent à faire parler d'elles. Or, loin de recueillir l'adhésion du plus grand nombre, elles attirent plutôt la méfiance, la suspicion et les critiques, en particulier de la communauté de l'ESS, qui les perçoit comme à l'opposé de leurs valeurs et préoccupations. De leur côté, les défenseurs des monnaies virtuelles décentralisées ont une vision très stéréotypée des monnaies locales et SELs. Partant du fait que les premières circulent essentiellement sous forme papier, et en communauté restreinte et pour des usages très réduits pour les secondes, ils sont très sceptiques quant au pouvoir de transformation systémique de ces monnaies. Ces deux communautés semblent donc très opposées. Dans cet article, nous proposons une analyse remettant en cause cette vision. En effet, après avoir procédé à une clarification de ce que sont initialement les crypto-monnaies, les avoir mises en perspectives avec les monnaies locales et les SELs, et avoir présenté leurs évolutions techniques et théoriques débouchant sur une grande diversité depuis l'arrivée du Bitcoin, nous proposons une étude critique de certaines d'entre elles qui proposent des protocoles plus économes en énergie, basés sur des principes plus coopératifs et utiles à la collectivité et d'autres qui se mettent désormais au service de projets ancrés dans l'ESS. Les crypto-monnaies offrent des possibilités d'expansion et d'autonomie vis-à-vis du système standard en cumulant certaines forces transformatrices des SELs et des monnaies locales. Le caractère décentralisé de leur création et gestion des transactions les rend par ailleurs moins contrôlables par les autorités. Si celles-ci parviennent à fédérer les communautés de la philosophie open source et des crypto-monnaies et celles relevant des champs de l'ESS, elles pourraient impulser un mouvement d'une ampleur suffisante pour représenter un véritable contre-pouvoir et amorcer un changement systémique. En offrant une possibilité de création d'unités monétaires en dehors du système bancaire et du contrôle des autorités monétaires, autrement que par le crédit et donc de la dette, les monnaies virtuelles peuvent contribuer à la réappropriation de la monnaie par les citoyens. Elles offrent également l'espoir de lever la contrainte de financement qui limite si grandement l'essor de nombreuses activités, notamment celles à but non lucratif, relevant de l'ESS. En mettant les nouvelles innovations au service de communautés porteuses de valeurs de solidarité, de partage et de respect de l'environnement, les monnaies virtuelles pourraient bien provoquer un changement radical dans les structures productives et les rapports de force actuels, en donnant véritablement et directement le pouvoir de création monétaire aux citoyens. La seule chose freinant leur adoption est la confiance et le degré d'ouverture des consciences. Bien sûr des problèmes techniques et théoriques restent encore à régler. Nous ne sommes qu'à l'aube de ce qu'il sera possible de faire dans quelques années. Comme nous l'avons proposé dans la fin de l'article, de nouvelles fonctionnalités pourraient être ajoutées, comme une fonte géographique, rendue possible grâce à la géolocalisation des transactions, proposant une définition du local plus pertinente que celle basée sur des zones administratives. Cependant, tant que les individus ne s'autorisent pas à croire qu'une liberté monétaire est possible, qu'elle est déjà accessible par les crypto-monnaies, alors leur expansion et adoption restera limitée. Mais si la croissance et la diversification

de ce type de projets continuent à la même cadence, il se pourrait qu'elles deviennent très présentes au quotidien pour l'ensemble de la population, et finissent par faire une percée dans les mentalités. Des citoyens toujours plus nombreux pourraient ainsi s'en emparer et les modeler selon leurs choix. Et pour ce qui est de la confiance nécessaire à leur diffusion, Herlin (2015) conclut son ouvrage par ces quelques phrases, p.177: "*Si la confiance ne peut jamais exister à 100 %, il importe de bien évaluer les risques, et ils ne plaident pas en faveur du système actuel*." Bien évidemment, il y a de nouveaux défis techniques et théoriques à résoudre, il est donc important de continuer à innover en proposant des monnaies virtuelles décentralisées sécurisées dont certaines seront sans doute les dispositifs monétaires de demain.

BIBLIOGRAPHIE

Aglietta, Michel et André Orléan (2002). *La monnaie entre violence et confiance*, Paris, Odile Jacob, 384 pages.

Banque Centrale Européenne (2012). *Virtual Currency Schemes*, Frankfort, Banque centrale européenne, 55 pages.

Bentov, Iddo, Lee Charles, Mizrahi Alex et Rosenfeld Meni (2014). Proof of activity: extending Bitcoin's proof of work via proof of stake, *ACM SIGMETRICS Performance Evaluation Review*, vol. 42, n°38, pp. 34-37.

Bindewald, Leander, Maria Nginamau et Christophe Place (2013). Validating complementary and community currencies as an efficient tool for social and solidarity economy networking and development: the deployment of theory of change approach and evaluation standards for their impact assessment, présenté à l'UNRISD Conference « International Symposium on Potential and Limits of Social and Solidarity Economy », Genève, 6-8 mai.

Blanc, Jerôme (2011). Classifying "CCs": community, complementary and local currencies' types and generations, *International Journal of Community Currency Research*, vol. 15, pp. 4-10.

Blanc, Jérôme et Marie Fare (2012). Les monnaies sociales en tant que dispositifs innovants : une évaluation, *Innovations*, vol. 2, n°38, pp. 67-84.

Blanc, Jérôme (2015). Contester par projets. Le cas des monnaies locales associatives, *Revue de la régulation,* n°18.

Bode, Siglinde (2004). *Potentiale regionaler komplementar Währungen zur Förderung einer endogenen Regionalentwicklung*, Freie wissenschaftliche Arbeit zur Erlangung des Hochschulgrades einer Diplom Geographin, Universität Osnabrück, Fachbereich Kultur und Geowissenschaften, Osnabrück, 155 pages.

Bonneau, Joseph et Andrew Miller (2014). FawkesCoin: a cryptocurrency without public-key cryptography, dans Bruce Christianson, James Malcolm, Vashek Matyáš, Petr Švenda, Frank Stajano et Jonathan Anderson (sous la direction de), *Security Protocols XXII, 22nd International Workshop Cambridge*, Cham, Springer, pp. 359-370.

Cartelier, Jean (1991). Monnaie et système de paiement : le problème de la formation de l'équilibre, *Revue française d'économie*, vol. 6, n°3, pp. 3-37.

Cartelier, Jean (1996). *La monnaie*, Paris, Flammarion, 125 pages.

Chaum, David (1983). Blind signature system, dans David Chaum (sous la direction de), *Advances in Cryptology: Proceedings of Crypto*, New York et Londres, Plenum Press, p. 153.

De Vauplane, Hubert (2015). La fascination autour du Bitcoin et des « monnaies virtuelles » : comment les définir ?, Blog d'alternatives économiques, Internet, disponible à l'adresse URL : http://alternatives-economiques.fr/blogs/vauplane/2015/11/07/la-fascination-autour-du-bitcoin-et-des-%C2%AB-monnaies-virtuelles-%C2%BB-comment-les-definir/ (accédé le 30 janvier 2017).

Desmedt, Ludovic et Odile Lakomski-Laguerre (2016). Du Bitcoin au faircoin et au-delà, *Les dossiers d'Alternatives économiques*, n°006-05/2016, Internet, disponible à l'adresse URL : http://www.alternatives-economiques.fr/bitcoin-faircoin-dela/00067988 (accédé le 30 janvier 2017).

Dokhan, Julien (2000). Le temps contre l'argent : un SEL, *Socio-anthropologie*, vol. 7.

Dreier, Jannik, Ali Kassem et Pascal Lafourcade (2015). Formal analysis of e-cash protocols, dans Mohammad Obaidat, Pascal Lorenz, Pierangela Samarati (sous la direction de), *ICETE 2015 Proceedings of the 12th International Joint Conference on e-Business and Telecommunications*, vol. 4, Lisbonne, Scitepress, pp. 65-75.

Dumas, Jean-Guillaume, Pascal Lafourcade et Patrick Redon (2015). *Architectures PKI et communications sécurisées*, Paris, Dunod, 400 pages.

Dupré, Denis, Pierre-Yves Longaretti et Jean-Michel Servet (2015a). Fonctions valeurs et leviers d'une monnaie alternative pour une transition à la durabilité territoriale, présenté au 5ème congrès de l'Association Française d'Economie Politique (AFEP) « L'économie politique de l'entreprise : nouveaux enjeux, nouvelles perspectives », Lyon, 1-3 juillet.

Dupré, Denis, Pierre-Yves Longaretti et Jean-Michel Servet (2015b). Le Bitcoin contre la révolution des communs, présenté au 5ème congrès de l'Association Française d'Economie Politique (AFEP) « L'économie politique de l'entreprise : nouveaux enjeux, nouvelles perspectives », Lyon, 1-3 juillet.

Dziembowski, Stephan, Sébastien Faust, Vladimir Kolmogorov et Krysztof Pietrzak (2015). Proofs of space, dans Rosario Gennaro et Matthew Robshaw (sous la direction de), *Advances in Cryptology -- CRYPTO 2015: 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II*, Heidelberg, Springer, pp. 585-605.

Fievet, Cyril (2014). *Comprendre Bitcoin et les crypto-monnaies alternatives*, Paris, Librinova, 189 pages.

Gesell, Silvio (1948). *L'ordre économique naturel*, Paris, Issautier, 403 pages.

Hayek, Friedrich (1976). *Denationalisation of Money - the Argument Refined. An Analysis of the Theory and Practice of Concurrent Currencies*, Londres, The Institute of Economic Affairs, 146 pages.

Herlin, Philippe (2015). *Apple, Bitcoin, Paypal, Google: La fin des banques ? Comment la technologie va changer votre argent*, Paris, Eyrolles, 184 pages.

Ingham, Geoffrey (2004). *The Nature of Money*, Cambridge, Polity Press, 264 pages.

Kennedy, Margrit et Declan Kennedy (1995). *Interest and Inflation Free Money: Creating an Exchange Medium that Works for Everybody and Protects the Earth*, Philadelphie, New Society, 144 pages.

Kennedy, Magrit et Bernard Lietaer (2004). *Regionalwährungen: Neue Wege zu nachhaltigem Wohlstand*, Munich, Riemann, 304 pages.

Keynes, John Maynard (1930/1971). *A Treatise on Money*, vol. I, *The Pure Theory of Money*, dans Maurice Dobb et Pierro Sraffa (sous la direction de), *The Collected Writings of J.M. Keynes*, vol. V, Londres, Macmillan, 364 pages.

King, Sunny (2013). Primecoin: cryptocurrency with prime number proof-of-work, Internet, disponible à l'adresse URL : http://primecoin.io/bin/primecoin-paper.pdf (accédé le 31 janvier 2017).

King, Sunny et Scott Nadal (2012). PPCoin: peer-to-peer crypto-currency with proof-of-stake, Internet, disponible à l'adresse URL : http://peercoin.net/assets/paper/peercoin-paper.pdf (accédé le 31 janvier 2017).

Laacher, Smaïn (1998). L'État et les systèmes d'échanges locaux (SEL). Tensions et intentions à propos des notions de solidarité et d'intérêt général, *Politix*, vol. 11, n°42, pp. 123-149.

Laacher, Smaïn (2002). Les systèmes d'échange local (SEL) : entre utopie politique et réalisme économique, *Mouvements*, vol. 1, n°19, pp. 81-87.

Laborde, Stéphane (2015). *Théorie relative de la monnaie*, Licence publique générale GNU, 147 pages, Internet, disponible à l'adresse URL : http://trm.creationmonetaire.info/ (accédé le 31 janvier 2017).

Lakomski-Laguerre, Odile et Ludovic Desmedt (2015). L'alternative monétaire Bitcoin : une perspective institutionnaliste, *Revue de la régulation*, n°18.

Lamport, Leslie, Robert Shostak et Marshall Pease (1982). The byzantine generals problem, *ACM Transactions on Programming Languages and Systems*, vol. 4, n°3, pp. 382–401.

Laurent, Alain et Virginie Monvoisin (2015). Les nouvelles monnaies numériques : au-delà de la dématérialisation de la monnaie et de la contestation des banques, *Revue de la régulation*, n°18.

Lietaer, Bernard (2013). *Au cœur de la monnaie*, Gap, Yves Michel, 600 pages.

Martignoni, Jens (2012). A new approach to a typology of complementary currencies, *International Journal of Community Currency Research*, vol. 16, pp. 1-17.

Miller, Andrew, Ari Juels, Elaine Shi, Bryan Parno et Jonathan Katz (2014). Permacoin: Repurposing Bitcoin work for data preservation, dans *Proceedings of the 35th IEEE Symposium on Security and Privacy*, Los Alamitos CA, Conference Publishing Services, pp. 475-490.

Park, Sunoo, Krzysztof Pietrzak, Albert Kwon, Joël Alwen, Georg Fuchsbauer et Peter Gaži (2015). SpaceMint: a cryptocurrency based on proofs of space, disponible à l'adresse URL : https://eprint.iacr.org/2015/528.pdf (accédé le 24 janvier 2017).

Schroeder, Rolf, Yoshihisa Miyazaki et Marie Fare (2011). Community currency research: an analysis of the literature, *International Journal of Community Currency Research*, vol. 15, pp. 31-41.

Seyfang, Gill et Noel Longhurst (2013). Growing green money? Mapping community currencies for sustainable development, *Ecological Economics*, vol. 86, n°C, pp. 65–77.

Slay, Julia (2011). More than money: Literature review of the evidence base on Reciprocal Exchange Systems, *Nesta Discussion Paper,* 23 pages.

Théret, Bruno (sous la direction de) (2007). *La monnaie dévoilée par ses crises*, Paris, EHESS, 512 pages.

Tichit, Ariane, Clément Mathonnat et Diego Landivar (2016). Classifying non-bank currency systems using web data, *International Journal of Community Currency Research*, Vol. 20, pp. 1-16.

Tschorsch, Florian et Björn Scheuermann (2016). Bitcoin and beyond: a technical survey on decentralized digital currencies, *IEEE Communications Surveys and Tutorials*, vol. 18, n°3, pp. 2084-2123.

Weber, Beat (2014). Bitcoin and the legitimacy crisis of money. *Cambridge Journal of Economics*, vol. 40, n°1, pp. 17-41.

NOTES

1. http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32009L0110&from=FR, accédé le 8 janvier 2017.

2. Pour le détail de ces catégories voir BCE (2012) p.13-15.

3. https://le-coin-coin.fr/2900-le-bitcoin-et-les-communs-2/, accédé le 9 janvier 2017.

4. Jacques Favier est cofondateur et Secrétaire du Cercle du Coin. Normalien et agrégé d'Histoire, après un court passage par la Banque, il a eu une longue expérience dans l'investissement. Il contribue régulièrement comme auteur dans Les Echos.fr, Bitcoin.fr et le-coin-coin.fr.

5. http://alternatives-economiques.fr/blogs/vauplane/2015/11/07/la-fascination-autour-du-bitcoin-et-des-%C2%AB-monnaies-virtuelles-%C2%BB-comment-les-definir/, accédé le 9 janvier 2017.

6. Le Solviolette est la monnaie locale complémentaire de Toulouse. Elle a vu le jour en 2011. C'est une monnaie de type "Sol" c'est-à-dire développée en partie grâce au soutien d'une collectivité territoriale (ici la mairie de Toulouse).

7. Les auteurs utilisent ce terme pour désigner l'ensemble des monnaies dont la création et la circulation ne dépendent pas des établissements bancaires, ce qui est la plus petite caractéristique commune des monnaies dites "alternatives".

8. Il en est de même pour les SELs autorisant des négociations de rapports de valeurs entre les différents biens et services offerts dans le réseau. Il en résulte de même une simple comptabilisation de flux entre les participants dont la somme s'annule.

9. https://fr.wikipedia.org/wiki/Bitcoin#/media/File:Bitcoin_usd_price.png accéder le 12 janvier 2017

10. Organe de supervision français de la banque et de l'assurance.

11. La loi du 7 octobre 2016 pour une République numérique modifie l'article 521-3 du Code monétaire et financier et assouplit les conditions d'autorisation de développement d'un système de paiement numérique sans déclaration préalable nécessaire à l'ACPR. Ceci devrait faciliter la dématérialisation des monnaies locales et conséquemment leur essor.

12. http://www.lefigaro.fr/conjoncture/2015/06/17/20002-20150617ARTFIG00368-les-grecs-se-tournent-vers-la-monnaie-virtuelle.php, accédé le 24 janvier 2017.

13. http://www.ibtimes.co.uk/bitcoin-now-accepted-by-100000-merchants-worldwide-1486613, accédé le 24 janvier 2017.

14. https://www.shiftpayments.com/card, accédé le 24 janvier 2017.

15. https://prypto.com/, accédé le 24 janvier 2017.

16. https://www.coinbase.com, accédé le 24 janvier 2017.

17. Pour plus de détails techniques, voir Dumas *et al.*, 2015.

18. http://www.canardcoincoin.com/ou-acheter-une-crypto-monnaie-specifique/, accédé le 9 Janvier 2017.

19. Selon Fievet (2014), p.20, rien qu'à l'été 2014, entre juin et août 400 nouveaux Altcoins auraient vu le jour.

20. http://guncoin.info/about-guncoin/ accédé le 9 Janvier 2017.
21. http://www.potcoin.com/ accédé le 9 Janvier 2017.
22. http://dogecoin.com, accédé le 13 Janvier 2017.
23. https://litecoin.org/fr, accédé le 13 Janvier 2017.
24. http://primecoin.io, accédé le 9 Janvier 2017.
25. http://www.gridcoin.us, accédé le 9 Janvier 2017.
26. https://www.curecoin.net, accédé le 9 Janvier 2017.
27. http://foldingcoin.net/the-coin, accédé le 9 Janvier 2017.
28. https://peercoin.net, accédé le 9 Janvier 2017.
29. Pour une présentation détaillée de l'objectif de hachage voir Dumas *et al.* (2015).
30. https://github.com/input-output-hk/Scorex/wiki/Permacoin-Implementation, accédé le 13 Janvier 2017.
31. https://fr.burst-team.us/, accédé le 13 janvier 2017.
32. https://reporterre.net/Voleur-de-banques-en-cavale-Enric-Duran-prepare-un-nouveau-monde, accédé le 24 janvier 2017.
33. http://www.lemonde.fr/pixels/article/2014/11/28/le-faircoin-une-monnaie-en-ligne-equitable-au-service-des-cooperatives_4530892_4408996.html, accédé le 25 janvier 2017.
34. https://fair-coin.org/faircoin2.html accédé le 17 janvier 2017.
35. Une analyse critique de cette théorie et de sa mise en oeuvre dépasse le cadre de cet article et fait l'objet d'un document de travail en cours spécifiquement dédié à cela.
36. https://en.duniter.org/theoretical/#afreeeconomy, accédé le 17 janvier 2017.
37. http://fr.duniter.org/faq/#commentsassurerquepersonnenetricheenpossdantplusieurscomptes, accédé le 28 Janvier 2017.
38. Faircoin n'est pas une monnaie libre, mais en partage certaines caractéristiques.
39. http://www.le-sou.org/, accédé le 30 janvier 2017.
40. Par exemple la Doume dans le Puy-de-Dôme.

RÉSUMÉS

Dans cet article nous défendons l'idée que les monnaies virtuelles décentralisées peuvent contribuer au changement systémique impulsé par l'ESS. Nous montrons tout d'abord qu'elles cumulent en effet des points forts des monnaies locales et des SELs dans leur pouvoir transformateur et apportent des solutions à certaines de leurs faiblesses, tout en ayant évidemment leurs propres limites. Ensuite, nous soulignons qu'une grande diversification est en cours au sein des crypto-monnaies et que certaines d'entre elles développent désormais des protocoles économes en énergie plus utiles à la collectivité ou basés sur la coopération, alors que d'autres se mettent au service de projets à valeurs proches de l'ESS. Ceci pourrait fédérer deux courants qui pour le moment s'opposent sur les valeurs et ainsi créer un mouvement d'une ampleur suffisante pour représenter un véritable contre-pouvoir face aux structures dominantes. Nous émettons toutefois des critiques sur ces dispositifs et proposons, en dernier lieu, une idée de crypto-monnaie géolocalisée avec fonte qui pourrait répondre à certaines limites rencontrées notamment par les monnaies locales dans leur définition de la proximité.

In this paper we argue that decentralized virtual currencies can contribute to systemic change driven by SSE. We first show that they cumulate a number of the strengths of local currencies

and SELs in their transformative power and provide solutions to some of their weaknesses, while obviously having their own limitations. Secondly, we emphasize that there is a great diversification within crypto-currencies and that some of them are now developing energy-saving protocols that are more useful to the community or based on cooperation, while others serve projects close to SSE. The fusion of these projects, that have a priori opposed values, could therefore create a movement of sufficient magnitude to begin to represent a true counter-power. However, we have some criticisms of these devices and finally propose an idea of crypto-coin with geolocalized demurrage that could meet certain limits encountered especially by local currencies in their definition of proximity.

INDEX

Mots-clés : monnaies virtuelles décentralisées, crypto-monnaies, SELs, monnaies locales, innovations
Keywords : decentralized virtual currencies, crypto-currencies, LETs, social currencies, monetary

AUTEURS

ARIANE TICHIT

Maîtresse de conférences, Université Clermont Auvergne ariane.tichit@uca.fr

PASCAL LAFOURCADE

Maître de conférences HDR, Université Clermont Auvergne pascal.lafourcade@uca.fr

VINCENT MAZENOD

Ingénieur CNRS vincent.mazenod@uca.fr